Your search matched **14** of **940663** documents.

A maximum of **14** results are displayed, **25** to a page, sorted by **Relevance** in **descending** order.
You may refine your search by editing the current search expression or entering a new one the text box.

Then click **Search Again.**

(virtual private network) <and> Internet <and> servers

Search Again

Results:
Journal or Magazine = **JNL** Conference = **CNF** Standard = **STD**

1 **Agent information contracts within virtual private networks**
Aparicio, M., IV; Herman, P.; Stephens, W.; Jain, A.K.; Singh, M.P.;
High-Assurance Systems Engineering Symposium, 1998. Proceedings. Third IEEE International , 13-14 Nov 1998
Page(s): 304 -311

[Abstract] [PDF Full-Text (76 KB)] **IEEE CNF**

2 **An expanded NAT with server connection ability**
Eun-Sang Lee; Hyun-Seok Chae; Byoung-Soo Park; Myung-Ryul Choi;
TENCON 99. Proceedings of the IEEE Region 10 Conference , Volume: 2 , Dec 1999
Page(s): 1391 -1394 vol.2

[Abstract] [PDF Full-Text (256 KB)] **IEEE CNF**

3 **An information assurance architecture for army installations**

Hendy, T.; Troester, D.;
MILCOM 2000. 21st Century Military Communications Conference Proceedings , Volume: 1 , 2000
Page(s): 444 -448 vol.1

[Abstract] [PDF Full-Text (480 KB)] **IEEE CNF**

4 **Prototyping SIP-based VoIP services in Java**

Hua Zou; Hongman Wang; Wenxin Mao; Bai Wang; Focant, S.; Handekyn, K.; Chantrain, D.; Marly, N.;
Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on , Volume: 2 , 2000
Page(s): 1395 -1399 vol.2

[Abstract] [PDF Full-Text (344 KB)] **IEEE CNF**

---

5 **Mobile teleworking some solutions and information security aspects**
Hagn, C.; Markwitz, W.H.;
EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA , 2000
Page(s): 322 -325

[Abstract] [PDF Full-Text (264 KB)] **IEEE CNF**

---

6 **Design of a secure, intelligent, and reconfigurable Web cam using a C based system design flow**
Verkest, D.; Desmet, D.; Avasare, P.; Coene, P.; Decneut, S.; Hendrickx, F.; Marescaux, T.; Mignolet, J.-Y.; Pasko, R.; Schaumont, P.;
Signals, Systems and Computers, 2001. Conference Record of the Thirty-Fifth Asilomar Conference on , Volume: 1 , 2001
Page(s): 463 -467 vol.1

[Abstract] [PDF Full-Text (537 KB)] **IEEE CNF**

---

7 **Implementation of a flexible control system for launching stream services independently of the access network**
Lehtonen, R.; Heinonen, P.; Peltotalo, J.; Peltotalo, S.; Hara, V.; Harju, J.;
Service Portability and Virtual Customer Environments, 2000 IEEE , 2000
Page(s): 46 -51

[Abstract] [PDF Full-Text (636 KB)] **IEEE CNF**

---

8 **Policy-based hybrid management architecture for IP-based VPN**
Seung-Jin Baek; Moon-Sang Jeong; Jong-Tae Park; Tai-Myoung Chung;
Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP , 2000
Page(s): 987 -988

[Abstract] [PDF Full-Text (100 KB)] **IEEE CNF**

---

9 **A policy server for an access network (PSAN)**
Ogura, T.; Fukuda, K.; Iseda, K.; Okuda, M.;
Communications, 2001. ICC 2001. IEEE International Conference on , Volume: 8 , 2001
Page(s): 2404 -2409 vol.8

[Abstract] [PDF Full-Text (568 KB)] **IEEE CNF**

---

10 **CryptoManiac: a fast flexible architecture for secure communication**
Wu, L.; Weaver, C.; Austin, T.;
Computer Architecture, 2001. Proceedings. 28th Annual International Symposium on , 2001
Page(s): 110 -119

[Abstract] [PDF Full-Text (104 KB)] **IEEE CNF**

---

11 **Fault-tolerant virtual private networks within an autonomous system**
Junghee Han; Malan, G.R.; Jahanian, F.;
Reliable Distributed Systems, 2002. Proceedings. 21st IEEE Symposium on , 2002
Page(s): 41 -50

[Abstract] [PDF Full-Text (689 KB)] **IEEE CNF**

---

12 **IP security: what makes it work?**
Younglove, R.W.;
Computing & Control Engineering Journal , Volume: 12 Issue: 1 , Feb 2001
Page(s): 44 -46

[Abstract] [PDF Full-Text (320 KB)] **IEE JNL**

---

13 **Integrating wireless LAN and cellular data for the enterprise**
Hui Luo; Zhimei Jiang; Byoung-Jo Kim; Shankaranarayanan, N.K.; Henry, P.;
Internet Computing, IEEE , Volume: 7 Issue: 2 , Mar/Apr 2003
Page(s): 25 -33

[Abstract] [PDF Full-Text (315 KB)] **IEEE JNL**

14 **On demand network-wide VPN deployment in GPRS**
Xenakis, C.; Merakos, L.;
IEEE Network , Volume: 16 Issue: 6 , Nov/Dec 2002
Page(s): 28 -37

[Abstract] [PDF Full-Text (1553 KB)] **IEEE JNL**

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search
Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting
No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top

Policy-based hybrid management architecture for IP-based VPN

Seung-Jin Baek Moon-Sang Jeong Jong-Tae Park Tai-Myoung Chung
Sch. of Electron. & Electr. Eng., Kyungpook Nat. Univ., Taegu;

This paper appears in: **Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP**
04/10/2000 -04/14/2000, 2000
Location: Honolulu, HI , USA
On page(s): 987-988
2000
References Cited: 0
Number of Pages: xxvii+1022
INSPEC Accession Number: 6622435

Abstract:
This paper presents a policy-based hybrid management architecture for IP-based VPN (virtual private network) service that makes use of a centralized global policy management server

Index Terms:
Internet network servers network topology telecommunication network management IP-based VPN service centralized global policy management server policy-based hybrid management architecture virtual private network

Documents that cite this document
Select link to view other documents in the database that cite this one.

SEARCH RESULTS [PDF Full-Text (100 KB)] PREVIOUS NEXT
DOWNLOAD CITATION

VIRTUAL PRIVATE NETWORKS

D.Wood, V.Stoss, L.Chan-Lizardo, G.S.Papacostas, M.E.Stinson

AT&T and Philips Telecommunications UK Ltd., UK
AT&T Bell Laboratories, USA

INTRODUCTION

Virtual Private Networks is a concept that will have a significant impact on the future of business communications. The Virtual Private Network (VPN) offers a fresh, innovative approach to the traditional problem of supplying efficient, reliable, easy to use telecommunications for large, geographically dispersed groups of subscribers. VPN replaces existing private networks with a flexible architecture that is easily managed and at the same time provides enhanced services.

Today, private networks exist to allow the many locations of a company to communicate. This communication can be achieved via the PSTN but this has proved a limiting approach due to the length of full national numbers and the lack of in-dialling capabilities from the PSTN. The business is also typically subjected to undesirable delay, overhead, and expense when changes are needed to the service being provided.

One solution to this problem is for a business to build a private network by installing (or leasing from the PSTN operator) private trunks to interconnect all its Private Automated Branch Exchanges (PABXs). In this case, the PSTN is used only for calls to subscribers external to the private network. The private network will typically provide a private numbering plan and numerous other enhanced services not available on the PSTN. The disadvantage of this approach is that the business must obtain the necessary expertise to build and operate such a network and it tends to tie the business to a given technology which may become obsolete.

Further, as the number of business locations in the private network increases, so do the interconnect requirements and the network complexity. Traffic engineering and network management become more important and more costly. Indeed some large private networks can exceed the size and complexity of smaller PTTs.

It is here that the Virtual Private Network first shows its benefits allowing the private networks' operation to retain an apparently simple network without any loss of interconnect functionality.

THE VIRTUAL PRIVATE NETWORK (VPN) CONCEPT

Conceptually, in its simplest form, a VPN is a PSTN emulation of the dedicated private network. As such, it retains most of the advantages of the private network without the operational difficulties. The VPN uses the resources of the PSTN in a time-sharing fashion with other traffic, including other VPNs. Typically, the PABXs from the fully-fledged private network approach will remain, and the VPN will provide emulation of the private circuits that connect them. It is, however, also possible for individual lines or CENTREX groups to be included as part of the VPN.

The VPN provides the business with the features and flexibility of the private network, while leaving the maintenance and operational aspects to the PSTN operator. The time-sharing of network resources in a VPN results in overall savings due to the more efficient usage of facilities, the benefits of the combined engineering of facilities, and the economies of scale. These savings allow the public network operator to offer virtual network services at rates that are economically attractive to the end user yet still generate greater profit for the network operator than could be realised by leasing these circuits.

Additional benefits of replacing a private network with a VPN are increased reliability, flexibility, and performance. Studies have shown that typical public networks, through professional operation, maintenance, and administration, typically out-perform private networks. Apart from the access link, the resources available to a given customer are usually under software or database control implying that additional capacity or services can generally be provided more promptly by the network operator than can the provisioning of leased circuits. Additional features are also available through software control as opposed to the private network case where the user may have to upgrade software and/or hardware on a whole series of PABXs. Similarly, the VPN concept frees the users from some of the ties to existing dedicated technology - new features introduced on the VPN are available to the user immediately.

The flexible, time-shared nature of VPNs also allows the operator to construct VPNs for customers whose small size would otherwise make a private network uneconomic. Usage sensitive tariffs are also possible and these are likely to be especially attractive to such smaller customers.

USE OF INTELLIGENT NETWORK DATABASES (INDBs)

Information relating to the configuration of the VPN may either be distributed across the switching systems in the public network, or stored in one or more central databases, referred to as Intelligent Network DataBases (INDBs). Such VPNs are referred to respectively, as either "switch-based" or "INDB-based." The VPN INDB contains all the call handling and translation procedures. Because they have far greater potential for operating efficiencies and feature availability, this paper will concentrate on INDB-based VPNs.

The VPN switches are interconnected by a common channel signalling system with one or more of the switches designated as the Signal Transfer End Points (STEPs). These switches are the ones that communicate with the INDB. Therefore, if any VPN switch generates a request to route a VPN call, the request will access the INDB via these STEPs. An optional announcement and digit collection system can also be attached to any VPN switch on the network. This system allows customized announcements to be played over the network for various applications. Additionally if the call handling procedures so require, digit collection will be performed by this system.

In order to update the VPN network, a Database Management System (DBMS) is used to interface with the INDB. This system controls and maintains all changes to the INDB, including the addition of new VPN networks. The DBMS, with proper security measures, can also be provided to the customers allowing them to update their own networks.

The VPN call flow for an intra-VPN call in this scenario would be as follows (Figure 1):

- A VPN subscriber dials the number required.
- The VPN switch recognizes that this is a VPN call and formulates and sends a request to the INDB for number translation and other call processing information.
- The INDB, after executing necessary call processing routines, sends routing and billing information back to the VPN switch.
- The VPN switch routes the call to the appropriate destination according to the specified routing number and records the required call logging data.

Using an INDB separates the service from the networking and signalling. When the number of customers requiring VPN service is greater than one INDB can support, additional INDBs can be installed. Furthermore, these INDBs, through the use of proper signalling messages, can be used to provide other types of services, such as televoting, credit card calling, etc. By customizing the INDB, these additional services will be supported on the same network architecture.

ADDITIONAL SERVICE FEATURES

With the INDB in place, the flexibility and capability of Virtual Private Network service can be provided through a variety of service features as described in the following list.

Time and Day Routing. A VPN user or the telecommunications administration can direct calls to different destinations, or have them receive recorded announcements, depending on the time of day or the day of the week. For example, from Monday to Friday all calls go to the main business office, but at the weekend callers hear a recorded announcement asking them to call back on a weekday. Time and day may be used separately or together.

Command Routing. This feature allows the VPN user or the Telecommunications Administration to establish and activate destinations or define call treatments for calls arriving during an emergency or unanticipated conditions.

Customer Definable Numbering Plan. The VPN provides numbering facilities tailored to the individual customer's needs, including the ability for the customer to retain an existing private numbering scheme.

Closed User Groups. Stations in a VPN can establish sub-networks, called Closed User Groups within which the members of the closed user group can communicate. This is accomplished by mapping groups of originations to groups of destinations. Communications are permitted within the CUG but may or may not be permitted to or from external stations. A station can belong to multiple closed user groups. This feature helps VPN owners to control the use of their VPN facilities.

Intra VPN Calling. A station belonging to a VPN can call another station on the same VPN by using the customer's dialling plan.

As in a private network a VPN caller dials an extension number to reach another caller within the same VPN at the same location. To reach a user at a different location, but still within the same VPN, a caller dials an access code to identify the second location followed by the destination number.

Inter VPN Calling. A station in one VPN can call a station in another VPN by first dialling an access to identify the called VPN followed by the PABX and extension identification. In this case, the VPN station or the PABX may prefix the VPN identification to the dialed number. The VPN owner determines the VPNs with which he can communicate.

An example of this feature is a user on the VPN wishing to access a customer on a different VPN. The user would dial the customer's VPN identification code followed by the destination number.

Break-in to VPN from the Public Switched Telephone Network. Break-in is the capability that allows a caller to access the VPN from the public network. The caller must first dial a predetermined access code assigned to break-in calls to that particular VPN.

This feature allows a salesperson to call a station on the VPN of his company while on the road. The salesperson would first dial an access code to identify the VPN followed by the desired station number.

Break-out to the Public Switched Telephone Network from the VPN. Break-out is the situation when a VPN caller requires a PSTN number. This is achieved by dialling an access code for the PSTN followed by the public number.

This feature is similar to the Inter-VPN Calling feature. In this case, the PSTN has an identification code, similar to any other VPN, that the user must provide in order to access the Public Network. Alternately the user could dial a Public Network access code which is translated by the user's PABX into the Public Network identification code.

Authorisation Codes. This feature allows the station user to input a special authorisation code after dialling a call. This changes the restrictions associated with the originating station to those associated with the assigned

authorisation code. An announcement prompts the user to enter one or more digits. This prevents unauthorized use of facilities.

For example, consider the case of a business having stations with different restrictions at many locations. A user may attempt to call the personnel records computer from a station not allowed access to it. The VPN would recognize that this particular station does not have the authorisation to access the personnel data and will provide an announcement asking for authorisation to process the call. The user enters his authorisation code and after validation the VPN routes the call to the personnel records computer.

Virtual On-net Dialling. Virtual on-net dialling allows customers to incorporate stations not connected to the VPN into the VPN dialling plan. This station is called an off-net station. Users will dial the VPN number assigned to the off-net station to gain access to it, the off-net station appearing as if part of the VPN.

Private Network Interface. The customer can interface to any other private networks from the VPN.

For example, a business may have some locations that do not belong to the VPN, and these locations have their own private networks. In this case the VPN would be able to interface to the private networks.

Universal Access to Service. With this feature, a service that is available from offices at multiple locations across the private network can be obtained by dialling one network-wide number. On dialling the network-wide number, calls are routed to the nearest location.

For example, a company that offers a library or helpdesk service from different company locations, but not necessarily from all company locations, can use a single number to access these services. A user on the VPN would dial the service number and be connected to the services desk nearest to the user's location.

Customer Access to the Data Base Management System (DBMS). This feature allows VPN customers to access the DBMS to monitor and update their VPN networks. The capabilities provided through the DBMS include the reconfiguration of VPN call treatment, adding and deleting VPN locations, changing the dialling plans, updating the closed user groups, providing a series of alternate destinations, and receiving reports on various service related data.

Selective Call Logging. This feature allows a customer to select a subset of calls for which detailed call related data will be collected.

For example, a company may want to collect additional data on all calls that are made to the PSTN from the VPN.

Support for Supplementary Service. Supplementary services as defined by CCITT or Telecoms can be supported on the VPN. In the case of end-to- end services, the VPN will transparently carry messages used to invoke supplementary services, provided that the signalling systems used have the capability to support them.

While each of these features may be used separately, they can be combined to meet each VPN user's unique needs. Each feature is based on a discrete set of call processing instructions in the INDB. Associated with each set of instructions is a series of branches or call processing treatments corresponding to the different outcomes (e.g., time of day, day of week, etc.). By linking sets of instructions, a simple one-feature service can be set up, or a very complex service can be constructed. This set of features and administrative data associated with a service comprises a service provider record which can be changed via the DBMS System.

VPN SERVICE ADMINISTRATION

The use of centralized INDBs for VPN simplifies OA&M considerably. Since data related to the call handling procedures for VPN is centralized in one location, updates can be easily effected. The Telephone Administration need only update the database, and does not have to update every VPN switch individually. This considerably reduces the time needed to introduce a change in the VPN network and reduces operational and administration costs to the Telephone Administration.

The VPN INDB uses the DBMS that could be shared by both the Telephone Administration and by the VPN customer. By implementing the proper security measures, customers can be given access to the DBMS. The customer can update the VPN network to reflect changes in traffic patterns and traffic volume. Some of the changes that are possible include the creation of and modifications to closed user groups, altering the time of day / day of week routing patterns, and changing authorisation codes.

Individual control provides customers with many benefits. Firstly, the customer does not have to give up the control available with private networks. The customer has the same type of control in defining numbering plans, calling privileges, etc. as is available in private networks. Secondly, the customer is not limited to the size of the network. In a private network, if customer traffic changes dramatically, additional capital expenditure would be needed to modify the private network to accommodate these changes. Instead, on a VPN, the customer redefines the boundaries of the VPN network and allows the PSTN to absorb the changes in traffic patterns. Finally, if the customer has other services, such as Advanced Freephone, the same DBMS access facilities can be used to manage the database for those services.

WHO PROVIDES VPN SERVICES

Historically the circuits used in private networks have been supplied by the public network operators. Following this line, it is logical for public network operators to provide VPN services. The VPN can be carried on a special purpose overlay network or on the PSTN. The user then has the choice of the conventional private network or the VPN with the features and benefits discussed earlier, as costs and requirements dictate. The network operator must therefore balance the costs and benefits to determine his

pricing strategy.

In addition to the public switched telephone network there are also private switched networks run by governments and large businesses. Such networks can also be used to support VPNs. Thus a government network can support many departments, each defined as a VPN. This would give a centralised network operation, rather than each department having to run its own network, affording significant cost saving. The individual departments retain the freedom to configure their own networks thus avoiding the bureaucratic frustrations often associated with centralised control. A particular benefit is the local office where several departments within one building can utilise access to a single node of the network. In a similar way large businesses, especially conglomerates, may well use VPNs on their private switched networks.

An alternative type of private network providing VPN is the local business community. For example a major airport could provide a complete telecommunication infrastructure with each airline having a VPN to link its own departments, booking, check-ins, transit, cargo etc. together with break-in/break-out functions to external networks. A similar scenario can be envisioned in the business or science park, or even in the shopping mall.

The VPN services described above are based on a single supplier whether a public or private network. Businesses have a need to communicate over several networks whether internationally or across multi-network environments within a country. Networking of calls in a multi-vendor environment is well established but agreement on cooperative service is much more difficult to achieve. The INDB provides the ability to distinguish between the service and the network.

All information on a VPN is held in a single database which provides the service and instructs the network on how to route each call. The necessary interface between service and network must be defined either by the international standards bodies or by de-facto acceptance of vendor standards. It is certainly probable that such standards will be based on the emerging Transaction Capability designed for non-circuit related messages.

With such standards a single VPN service can be provided accross several networks giving businesses the communications that match the international nature of their operations.

SUMMARY

This paper has described some of the features and services available with Virtual Private Networks.

The benefits of VPN, as stated in this paper, are:

- The advantages of private networks, such as uniform numbering plan and calling privileges, are retained without many of the shortcomings.
- OA&M is performed by the Telephone Administration as the VPN is part of the PSTN, relieving the VPN customer of this burden.
- Changes to the customer network can be effected easily and quickly as the VPN is defined in the software of the PSTN.
- The VPN customer does not have to worry about equipment obsolesence.

These benefits are what makes VPN the attractive and economical alternative to the private network.

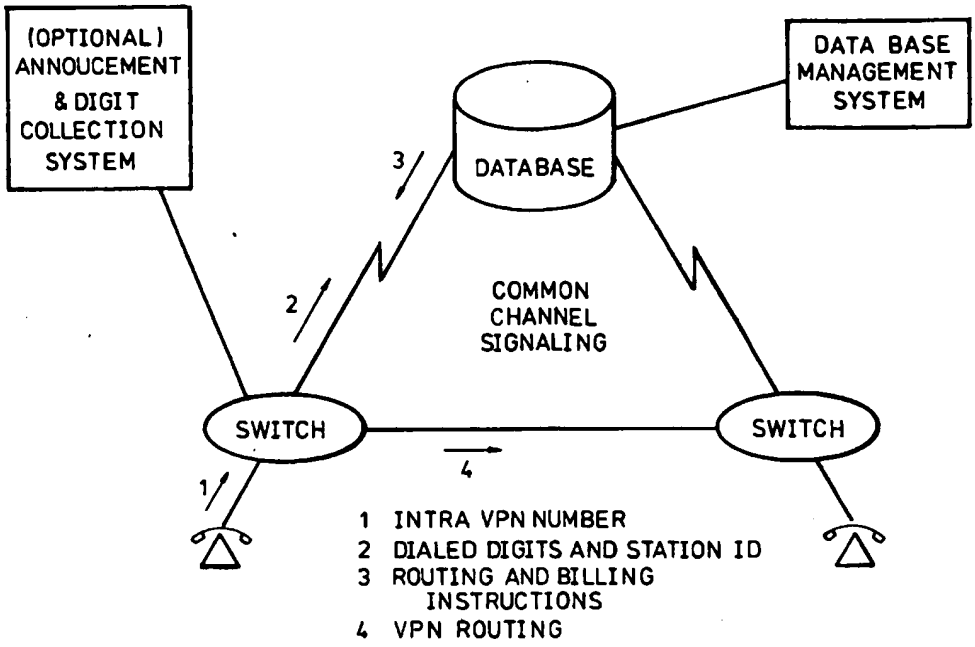

Figure 1 VPN Call Flow For Intra VPN Call